10210-0016260

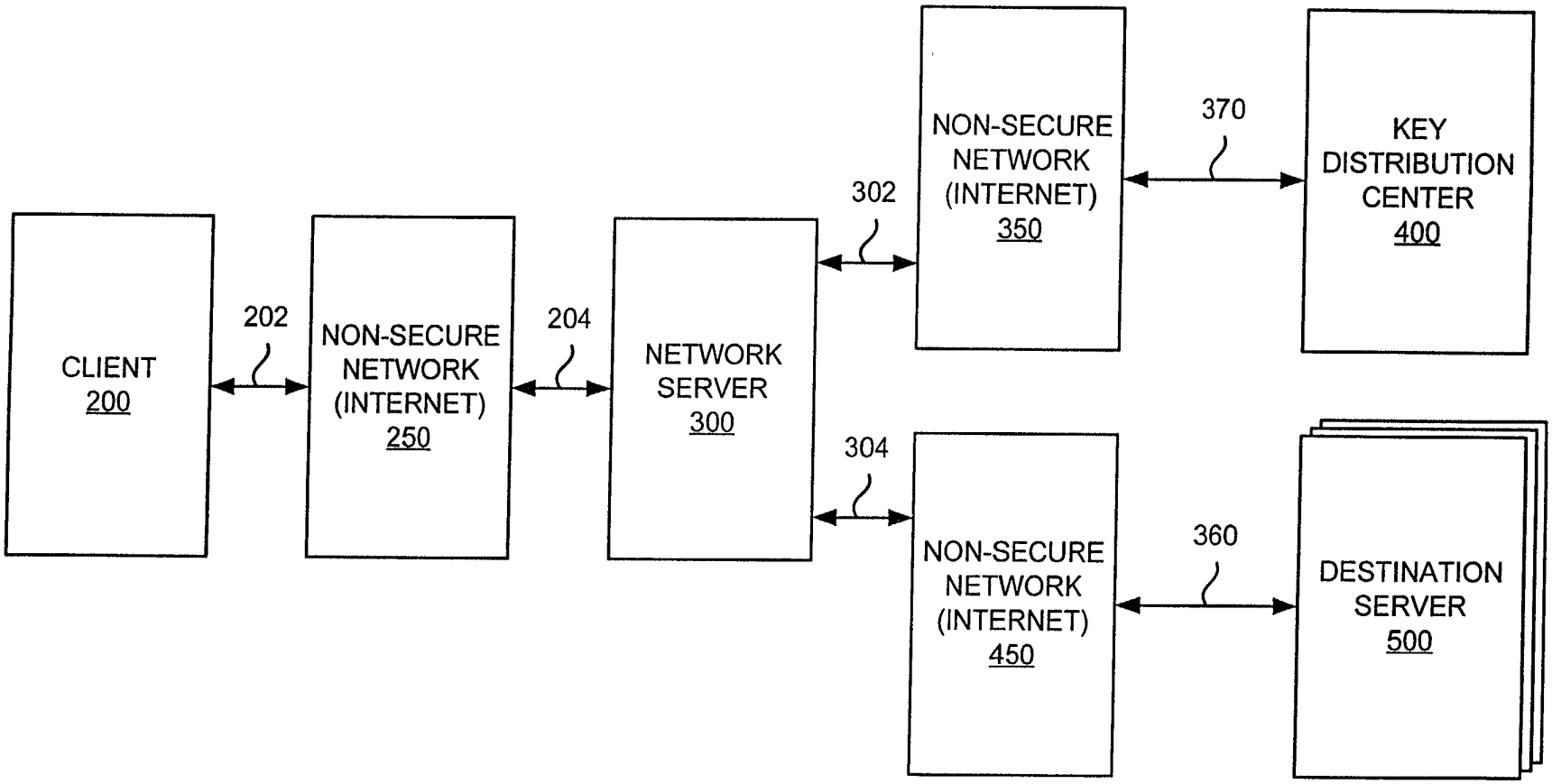


FIGURE 1

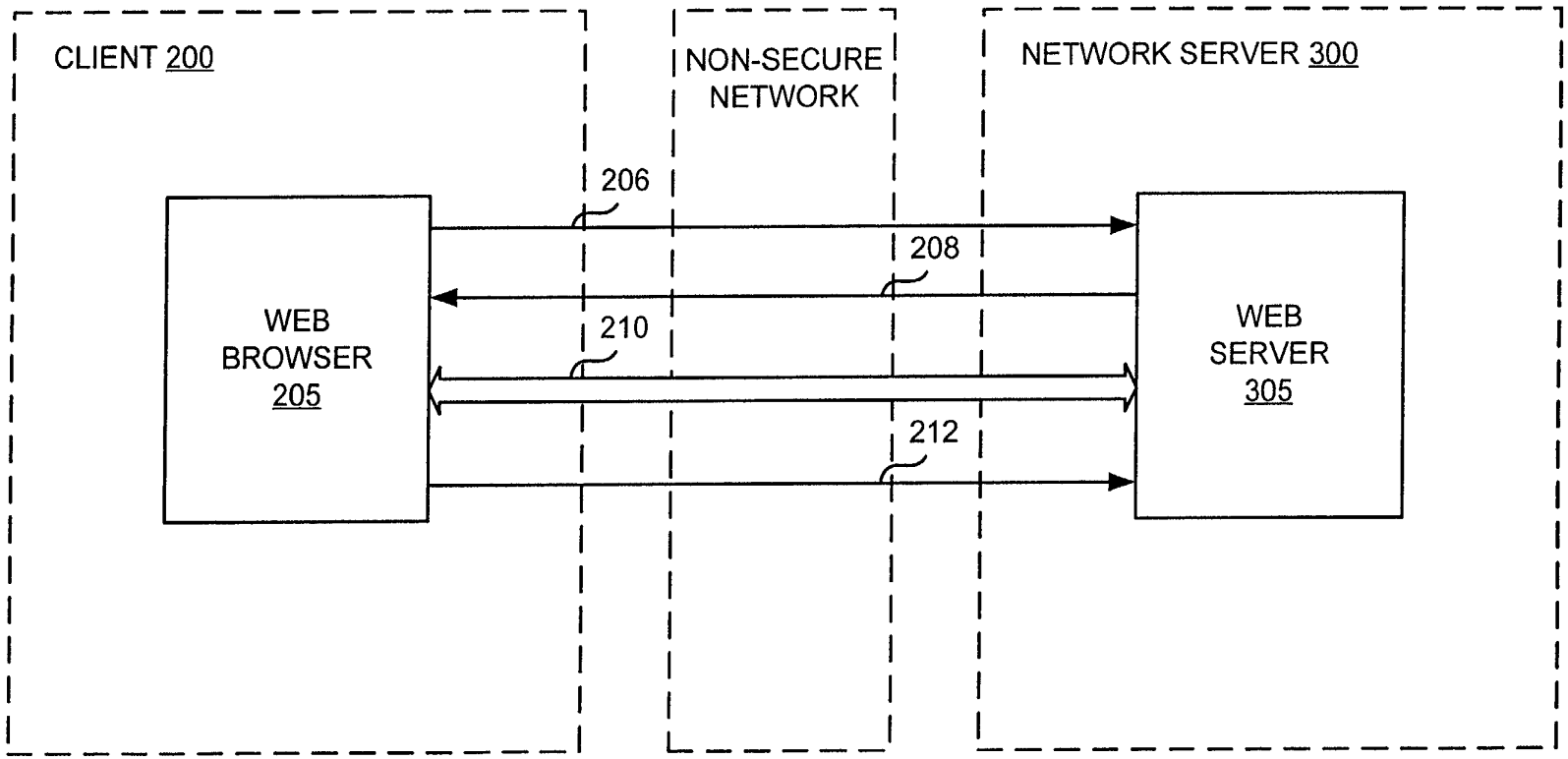

CLIENT 200
NON-SECURE NETWORK
NETWORK SERVER 300
206
208
210
212
WEB BROWSER 205
WEB SERVER 305

FIGURE 2

US 2010/0169260

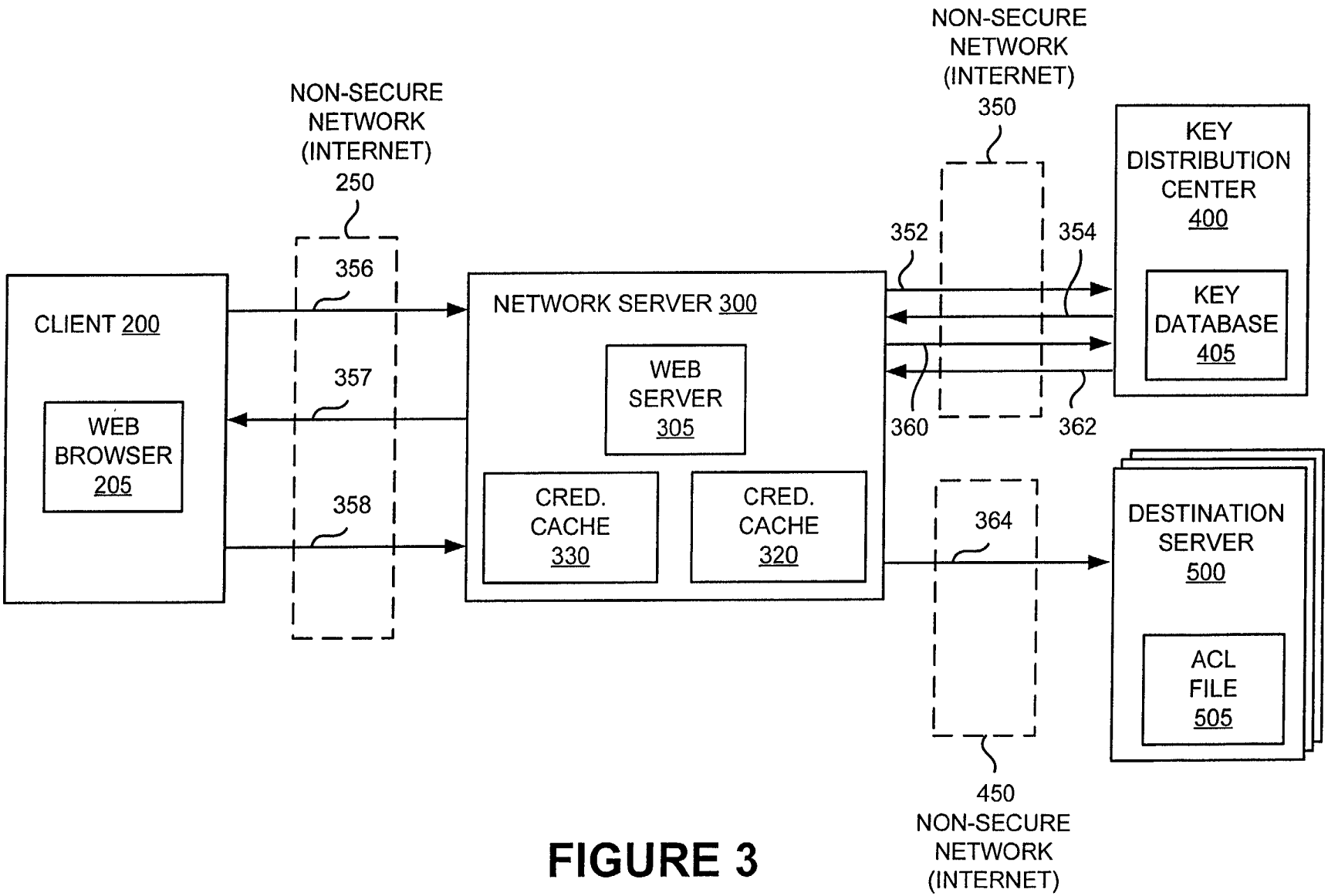


FIGURE 3

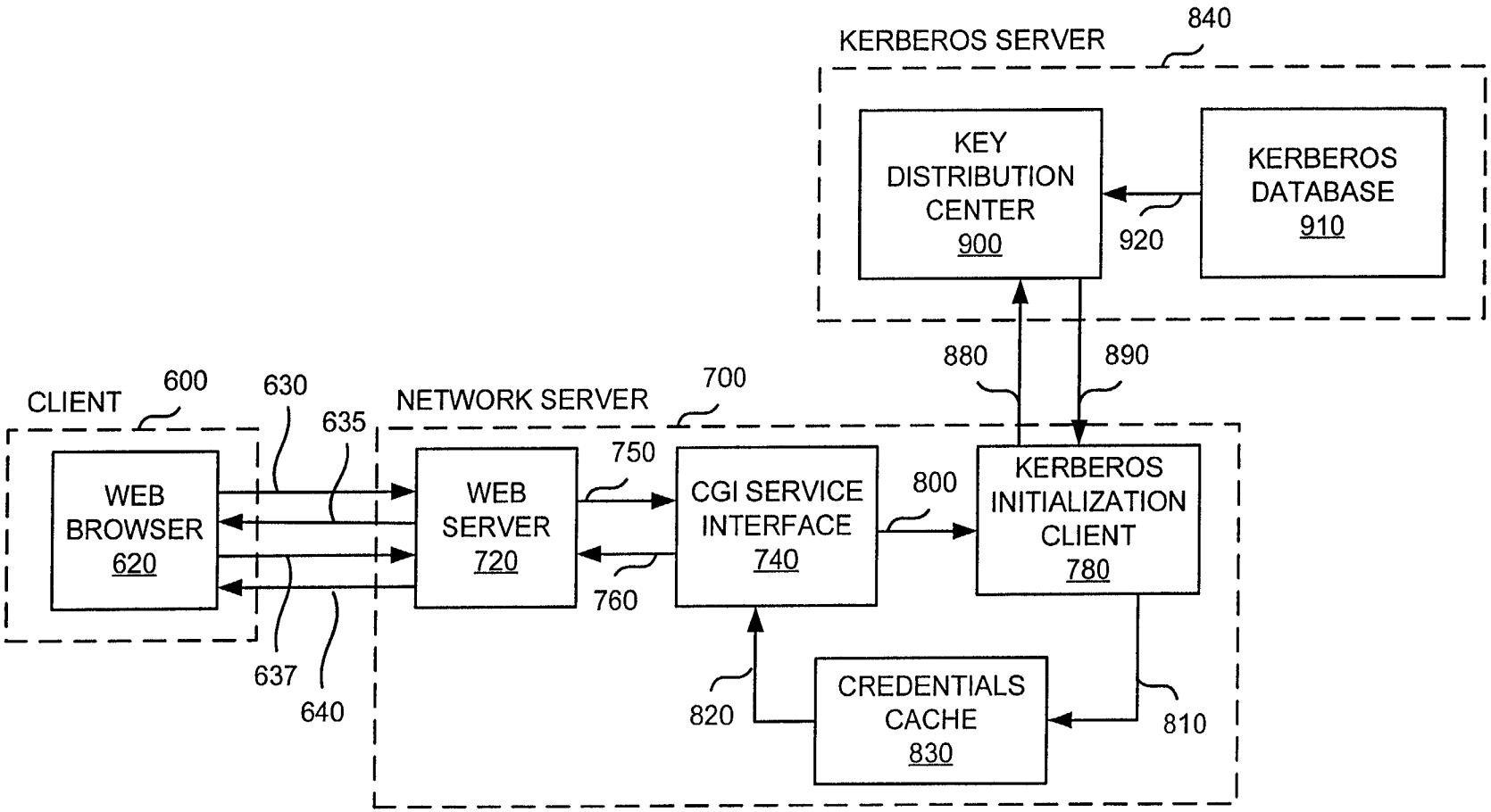

KERBEROS SERVER
840
KEY DISTRIBUTION CENTER 900
KERBEROS DATABASE 910
920
880
890
CLIENT
600
630
635
NETWORK SERVER
700
WEB BROWSER 620
WEB SERVER 720
750
760
CGI SERVICE INTERFACE 740
800
KERBEROS INITIALIZATION CLIENT 780
637
640
820
CREDENTIALS CACHE 830
810

FIGURE 4

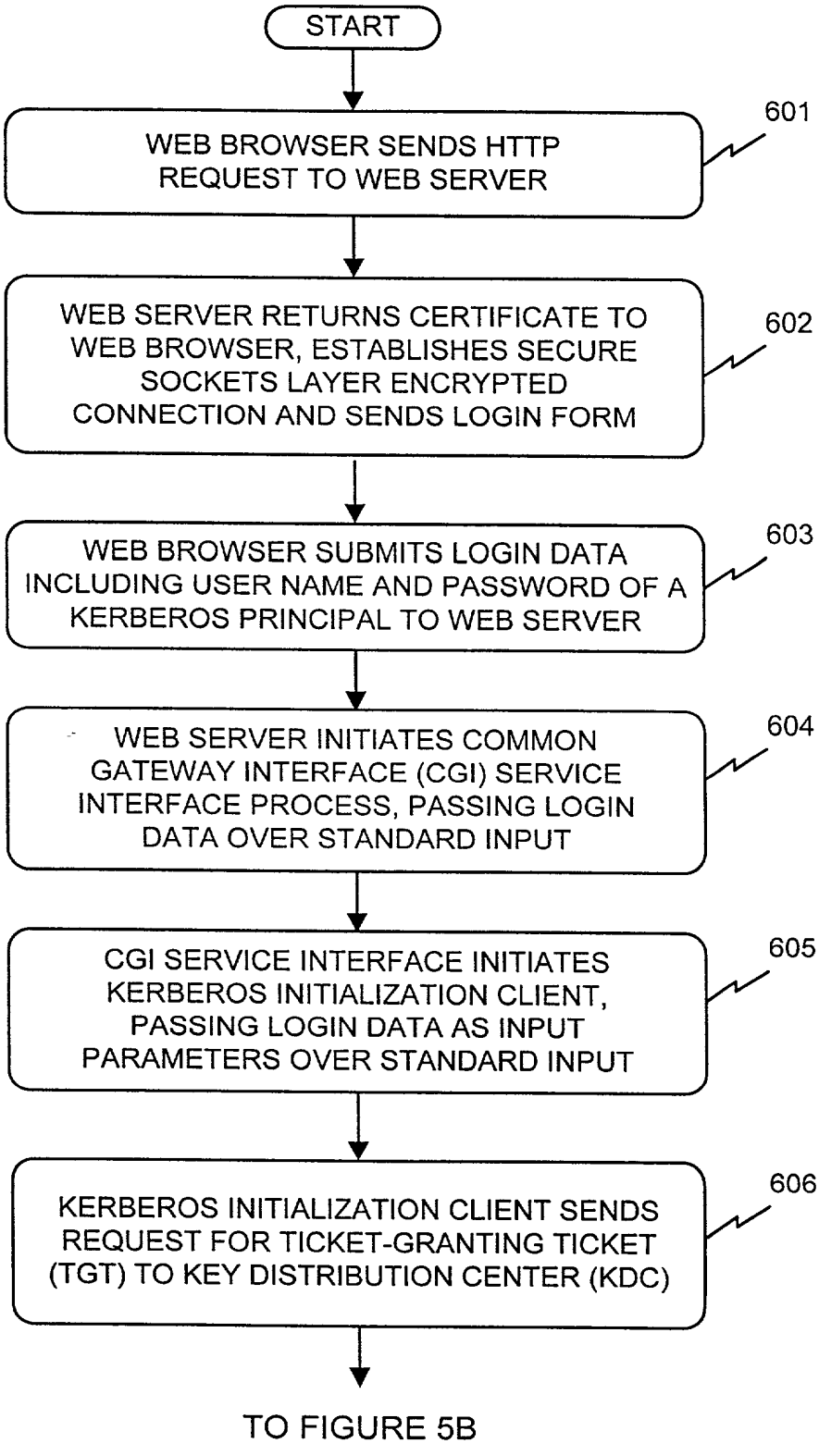

START
WEB BROWSER SENDS HTTP REQUEST TO WEB SERVER
601
WEB SERVER RETURNS CERTIFICATE TO WEB BROWSER, ESTABLISHES SECURE SOCKETS LAYER ENCRYPTED CONNECTION AND SENDS LOGIN FORM
602
WEB BROWSER SUBMITS LOGIN DATA INCLUDING USER NAME AND PASSWORD OF A KERBEROS PRINCIPAL TO WEB SERVER
603
WEB SERVER INITIATES COMMON GATEWAY INTERFACE (CGI) SERVICE INTERFACE PROCESS, PASSING LOGIN DATA OVER STANDARD INPUT
604
CGI SERVICE INTERFACE INITIATES KERBEROS INITIALIZATION CLIENT, PASSING LOGIN DATA AS INPUT PARAMETERS OVER STANDARD INPUT
605
KERBEROS INITIALIZATION CLIENT SENDS REQUEST FOR TICKET-GRANTING TICKET (TGT) TO KEY DISTRIBUTION CENTER (KDC)
606
TO FIGURE 5B

FIGURE 5A

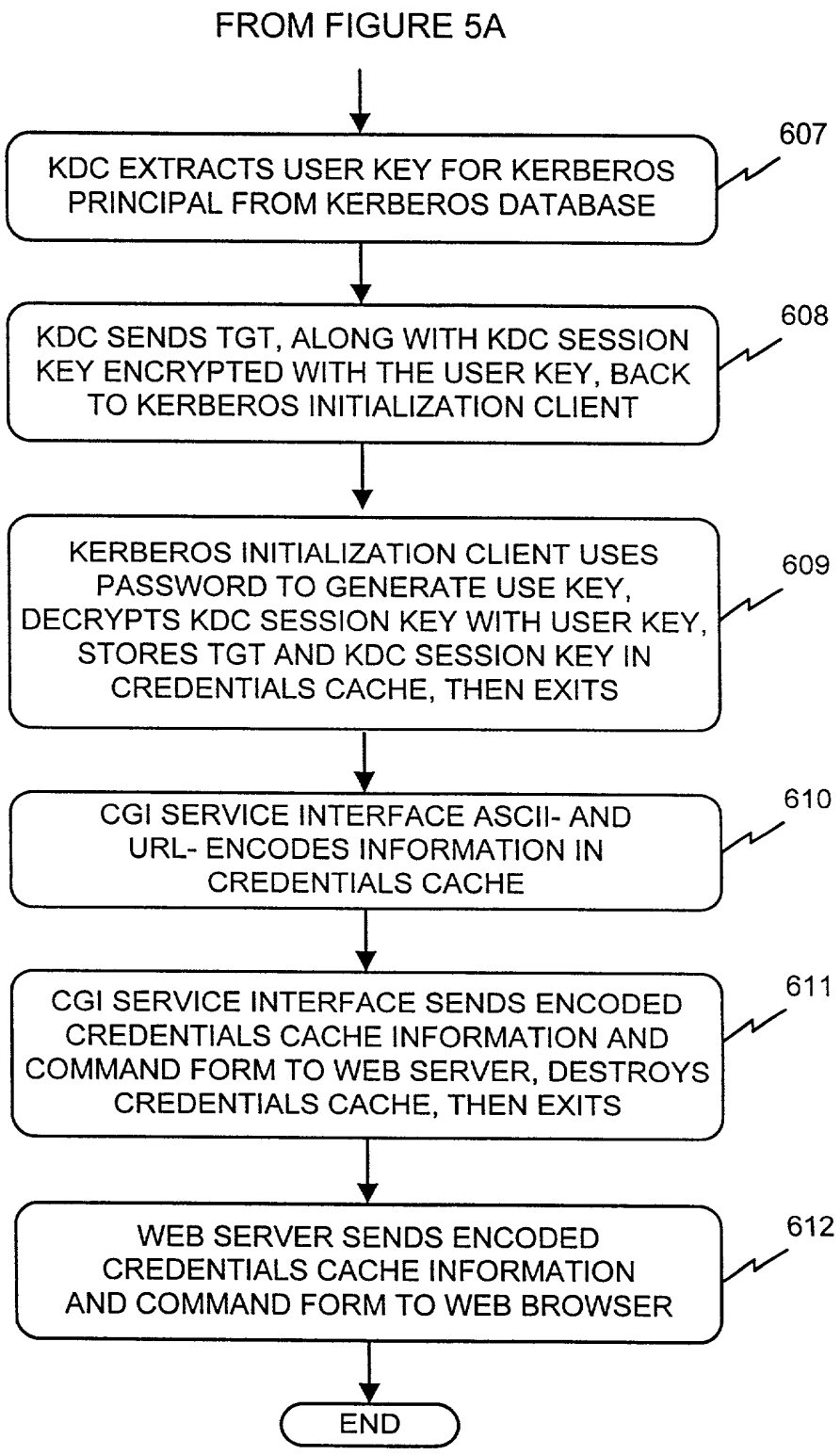
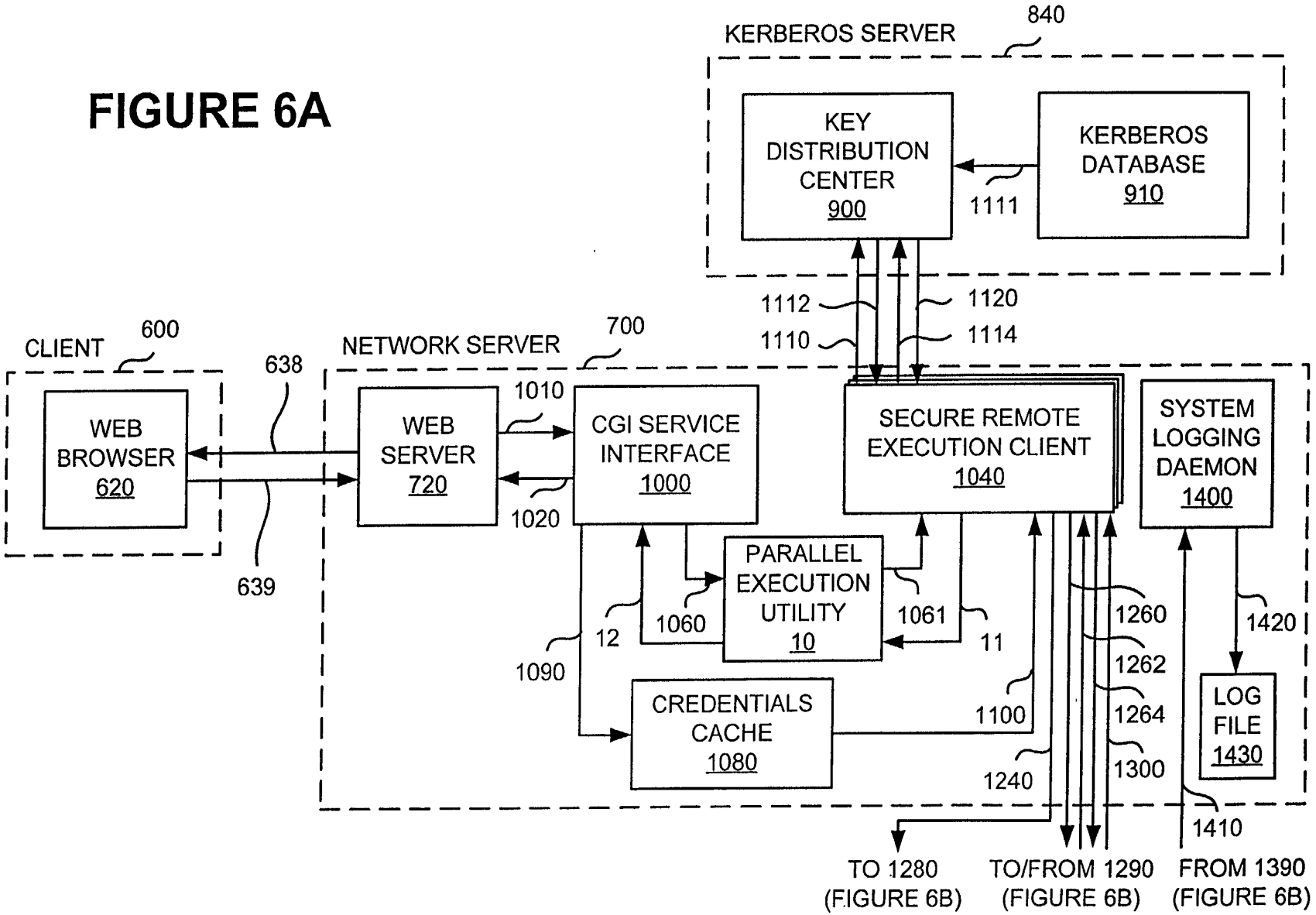

FROM FIGURE 5A
KDC EXTRACTS USER KEY FOR KERBEROS PRINCIPAL FROM KERBEROS DATABASE
607
KDC SENDS TGT, ALONG WITH KDC SESSION KEY ENCRYPTED WITH THE USER KEY, BACK TO KERBEROS INITIALIZATION CLIENT
608
KERBEROS INITIALIZATION CLIENT USES PASSWORD TO GENERATE USE KEY, DECRYPTS KDC SESSION KEY WITH USER KEY, STORES TGT AND KDC SESSION KEY IN CREDENTIALS CACHE, THEN EXITS
609
CGI SERVICE INTERFACE ASCII- AND URL- ENCODES INFORMATION IN CREDENTIALS CACHE
610
CGI SERVICE INTERFACE SENDS ENCODED CREDENTIALS CACHE INFORMATION AND COMMAND FORM TO WEB SERVER, DESTROYS CREDENTIALS CACHE, THEN EXITS
611
WEB SERVER SENDS ENCODED CREDENTIALS CACHE INFORMATION AND COMMAND FORM TO WEB BROWSER
612
END

FIGURE 5B

FIGURE 6A


KERBEROS SERVER
840
KEY DISTRIBUTION CENTER 900
KERBEROS DATABASE 910
1111
1112
1110
1120
1114
CLIENT
600
NETWORK SERVER
700
638
WEB BROWSER 620
WEB SERVER 720
1010
1020
CGI SERVICE INTERFACE 1000
SECURE REMOTE EXECUTION CLIENT 1040
SYSTEM LOGGING DAEMON 1400
639
PARALLEL EXECUTION UTILITY 10
1060
12
1061
11
1090
1260
1262
1264
1300
1420
CREDENTIALS CACHE 1080
1100
1240
LOG FILE 1430
1410
TO 1280 (FIGURE 6B)
TO/FROM 1290 (FIGURE 6B)
FROM 1390 (FIGURE 6B)

Docket 00165260

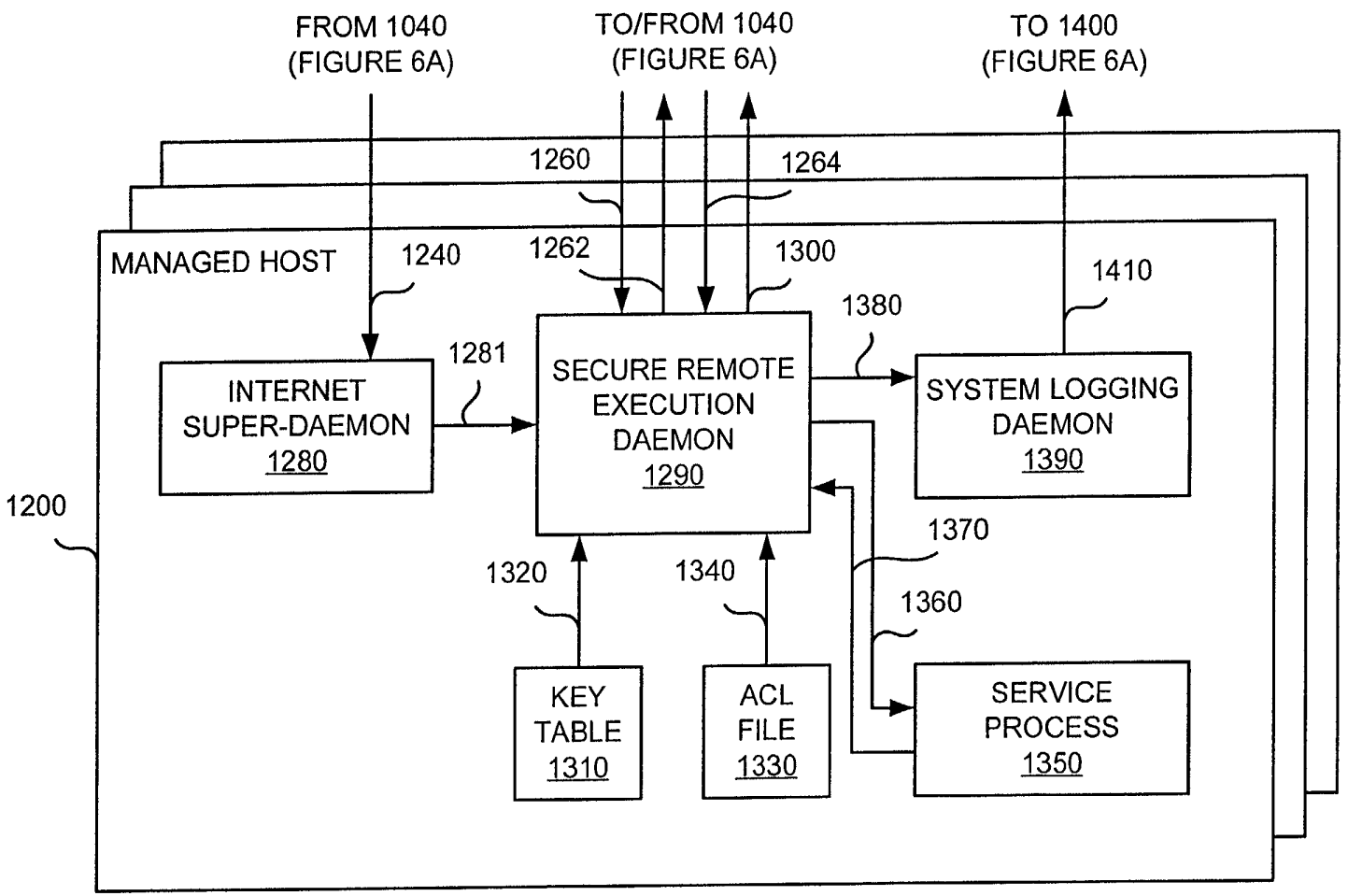


FIGURE 6B

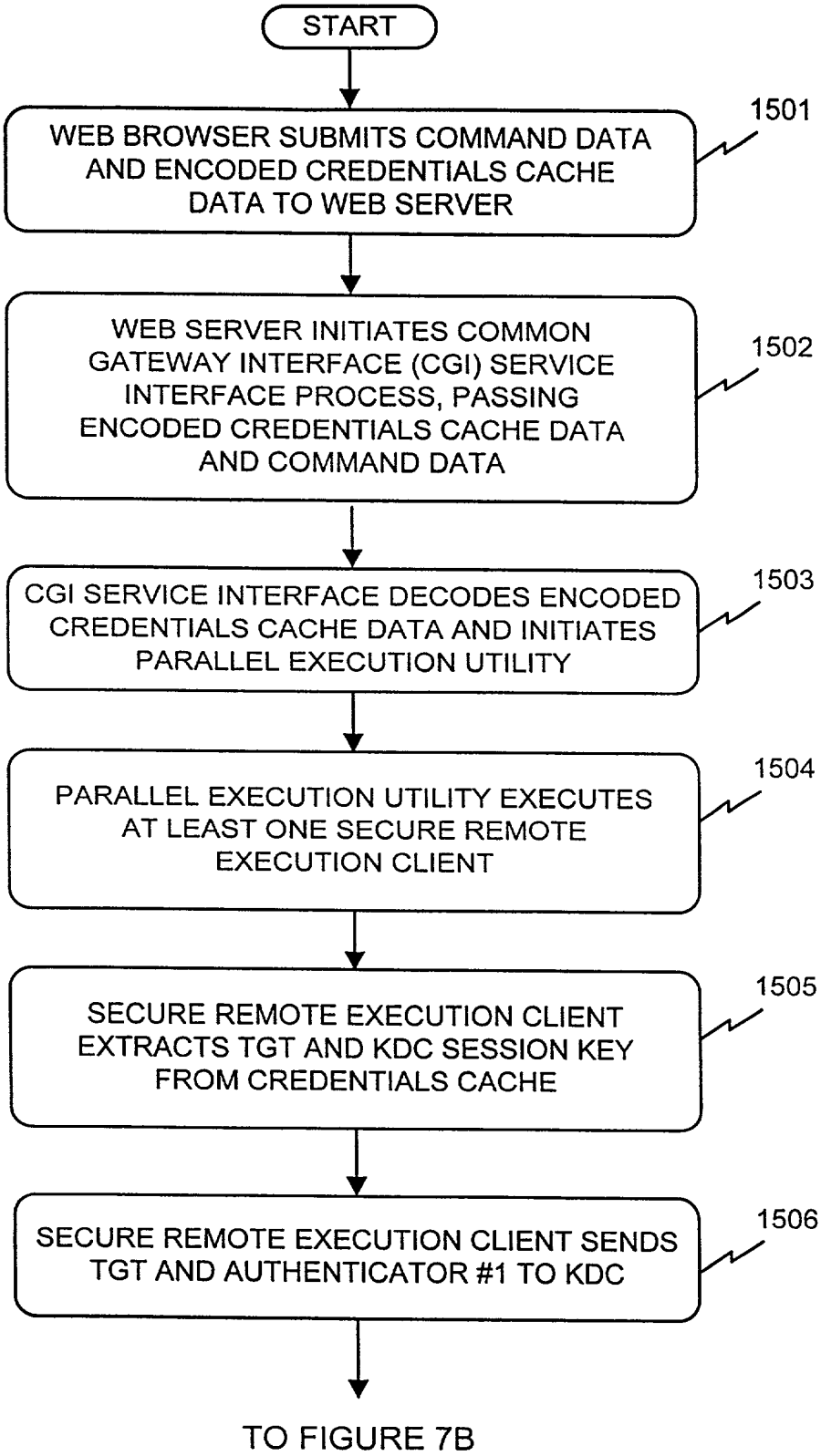

START
WEB BROWSER SUBMITS COMMAND DATA AND ENCODED CREDENTIALS CACHE DATA TO WEB SERVER
1501
WEB SERVER INITIATES COMMON GATEWAY INTERFACE (CGI) SERVICE INTERFACE PROCESS, PASSING ENCODED CREDENTIALS CACHE DATA AND COMMAND DATA
1502
CGI SERVICE INTERFACE DECODES ENCODED CREDENTIALS CACHE DATA AND INITIATES PARALLEL EXECUTION UTILITY
1503
PARALLEL EXECUTION UTILITY EXECUTES AT LEAST ONE SECURE REMOTE EXECUTION CLIENT
1504
SECURE REMOTE EXECUTION CLIENT EXTRACTS TGT AND KDC SESSION KEY FROM CREDENTIALS CACHE
1505
SECURE REMOTE EXECUTION CLIENT SENDS TGT AND AUTHENTICATOR #1 TO KDC
1506
TO FIGURE 7B

FIGURE 7A

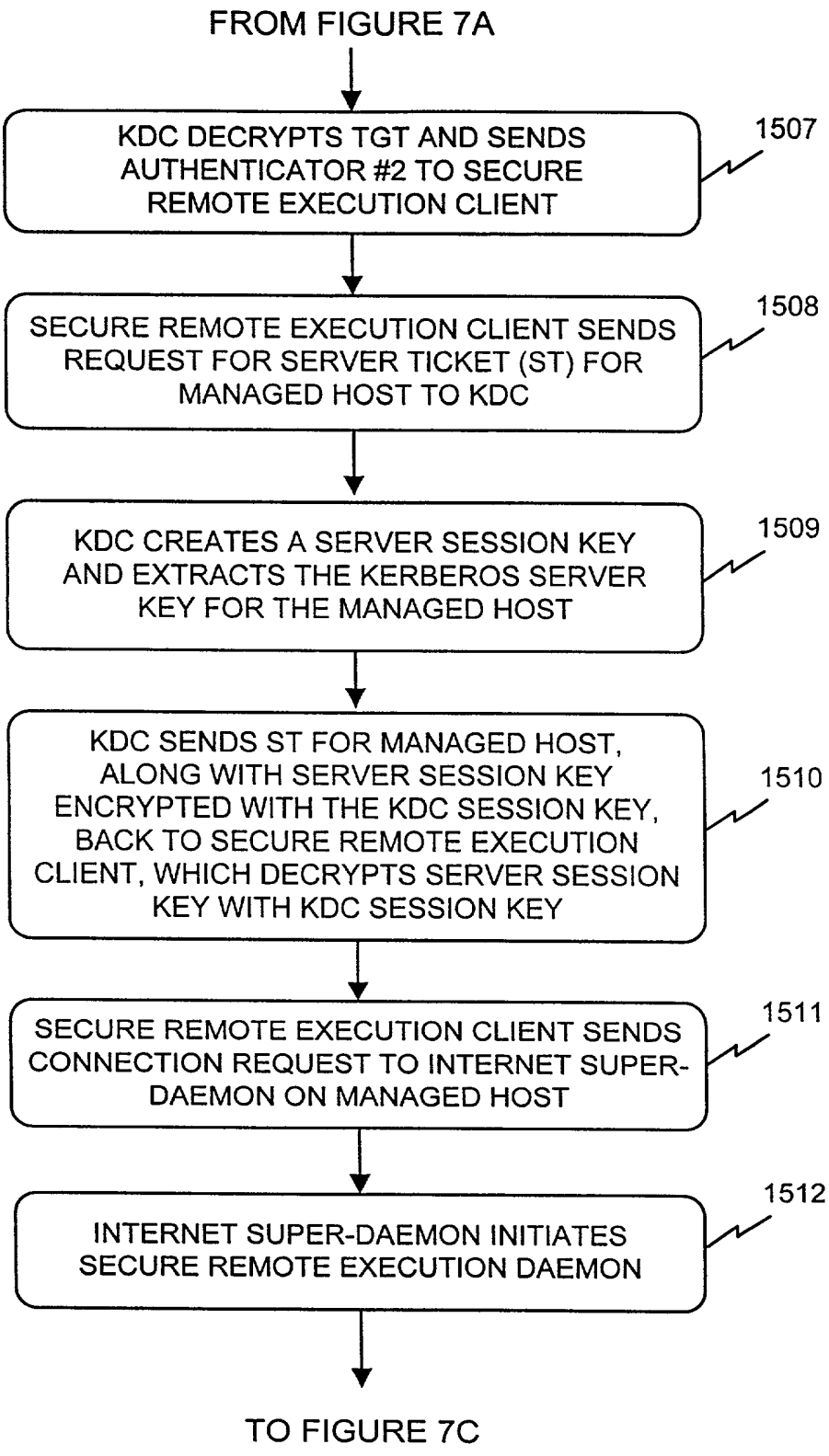

FROM FIGURE 7A
KDC DECRYPTS TGT AND SENDS AUTHENTICATOR #2 TO SECURE REMOTE EXECUTION CLIENT
1507
SECURE REMOTE EXECUTION CLIENT SENDS REQUEST FOR SERVER TICKET (ST) FOR MANAGED HOST TO KDC
1508
KDC CREATES A SERVER SESSION KEY AND EXTRACTS THE KERBEROS SERVER KEY FOR THE MANAGED HOST
1509
KDC SENDS ST FOR MANAGED HOST, ALONG WITH SERVER SESSION KEY ENCRYPTED WITH THE KDC SESSION KEY, BACK TO SECURE REMOTE EXECUTION CLIENT, WHICH DECRYPTS SERVER SESSION KEY WITH KDC SESSION KEY
1510
SECURE REMOTE EXECUTION CLIENT SENDS CONNECTION REQUEST TO INTERNET SUPER-DAEMON ON MANAGED HOST
1511
INTERNET SUPER-DAEMON INITIATES SECURE REMOTE EXECUTION DAEMON
1512
TO FIGURE 7C

FIGURE 7B

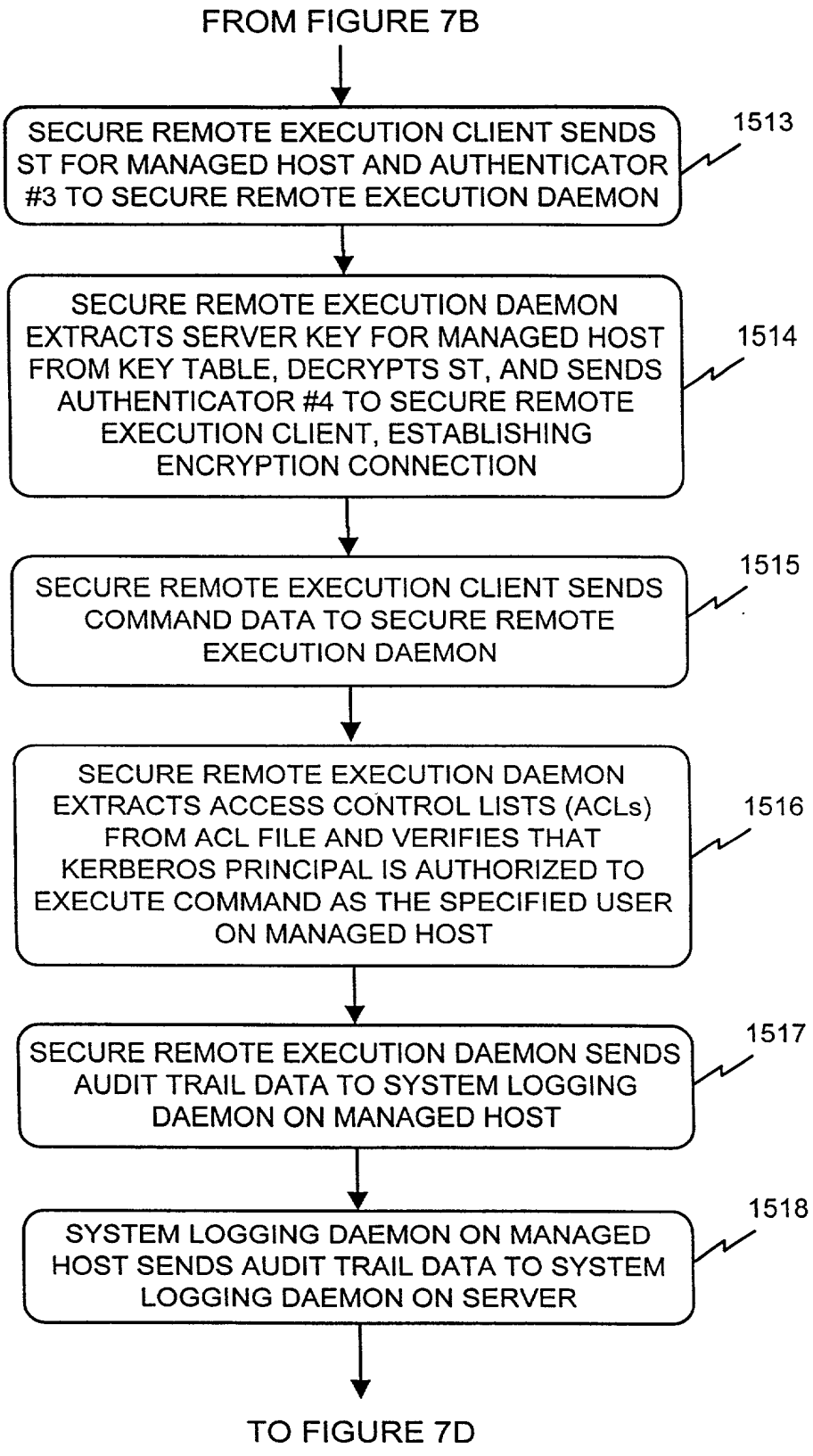

FROM FIGURE 7B
SECURE REMOTE EXECUTION CLIENT SENDS ST FOR MANAGED HOST AND AUTHENTICATOR #3 TO SECURE REMOTE EXECUTION DAEMON
1513
SECURE REMOTE EXECUTION DAEMON EXTRACTS SERVER KEY FOR MANAGED HOST FROM KEY TABLE, DECRYPTS ST, AND SENDS AUTHENTICATOR #4 TO SECURE REMOTE EXECUTION CLIENT, ESTABLISHING ENCRYPTION CONNECTION
1514
SECURE REMOTE EXECUTION CLIENT SENDS COMMAND DATA TO SECURE REMOTE EXECUTION DAEMON
1515
SECURE REMOTE EXECUTION DAEMON EXTRACTS ACCESS CONTROL LISTS (ACLs) FROM ACL FILE AND VERIFIES THAT KERBEROS PRINCIPAL IS AUTHORIZED TO EXECUTE COMMAND AS THE SPECIFIED USER ON MANAGED HOST
1516
SECURE REMOTE EXECUTION DAEMON SENDS AUDIT TRAIL DATA TO SYSTEM LOGGING DAEMON ON MANAGED HOST
1517
SYSTEM LOGGING DAEMON ON MANAGED HOST SENDS AUDIT TRAIL DATA TO SYSTEM LOGGING DAEMON ON SERVER
1518
TO FIGURE 7D

FIGURE 7C

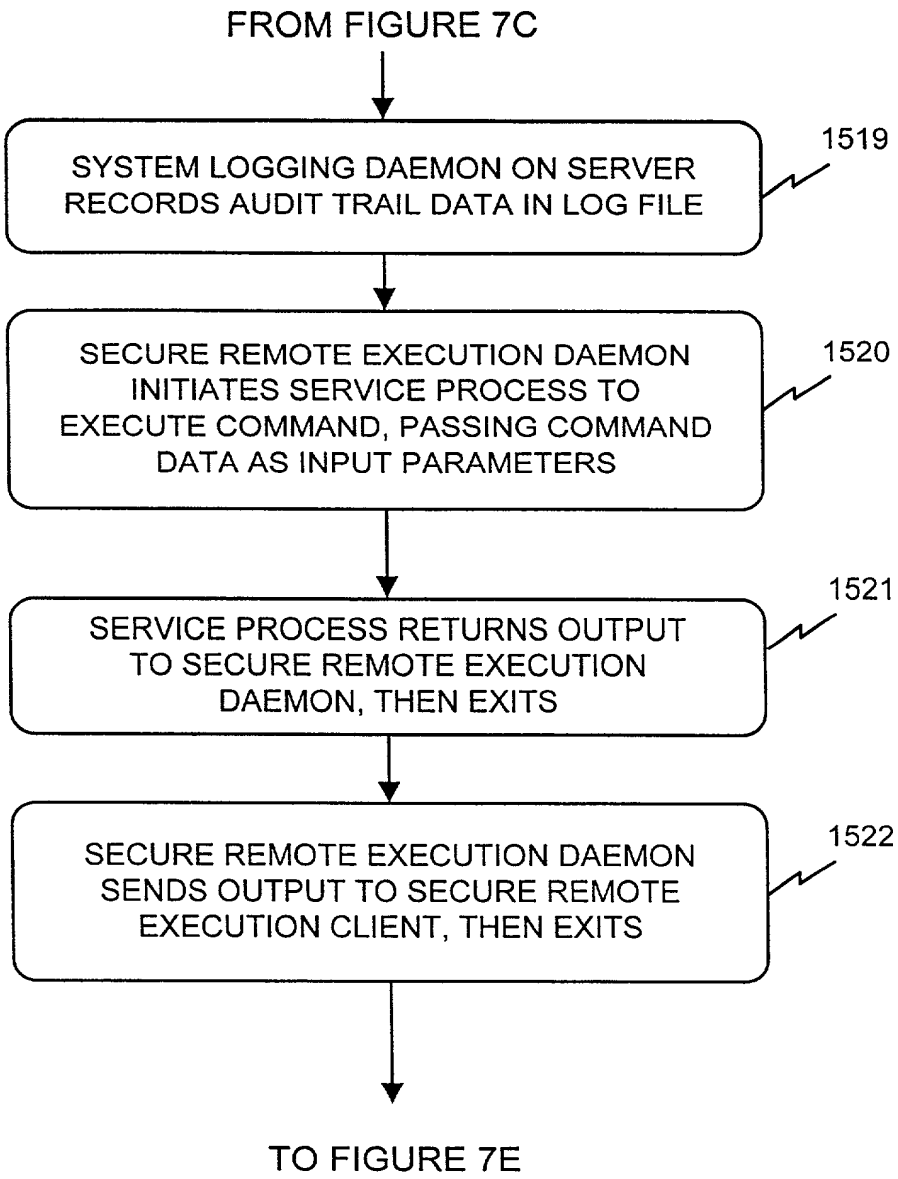

FROM FIGURE 7C
SYSTEM LOGGING DAEMON ON SERVER RECORDS AUDIT TRAIL DATA IN LOG FILE
1519
SECURE REMOTE EXECUTION DAEMON INITIATES SERVICE PROCESS TO EXECUTE COMMAND, PASSING COMMAND DATA AS INPUT PARAMETERS
1520
SERVICE PROCESS RETURNS OUTPUT TO SECURE REMOTE EXECUTION DAEMON, THEN EXITS
1521
SECURE REMOTE EXECUTION DAEMON SENDS OUTPUT TO SECURE REMOTE EXECUTION CLIENT, THEN EXITS
1522
TO FIGURE 7E

FIGURE 7D

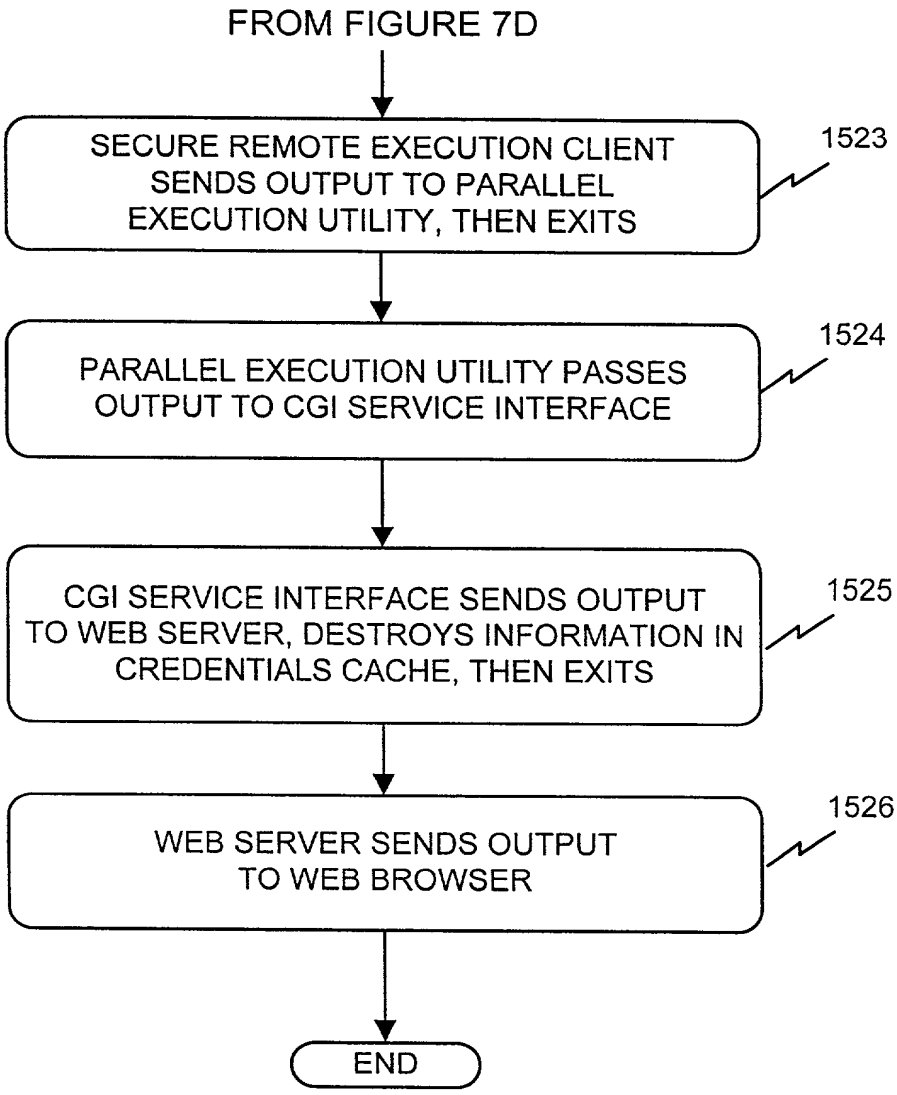

FROM FIGURE 7D
SECURE REMOTE EXECUTION CLIENT SENDS OUTPUT TO PARALLEL EXECUTION UTILITY, THEN EXITS
1523
PARALLEL EXECUTION UTILITY PASSES OUTPUT TO CGI SERVICE INTERFACE
1524
CGI SERVICE INTERFACE SENDS OUTPUT TO WEB SERVER, DESTROYS INFORMATION IN CREDENTIALS CACHE, THEN EXITS
1525
WEB SERVER SENDS OUTPUT TO WEB BROWSER
1526
END

FIGURE 7E

T021F0 00F65260

Fig. 8

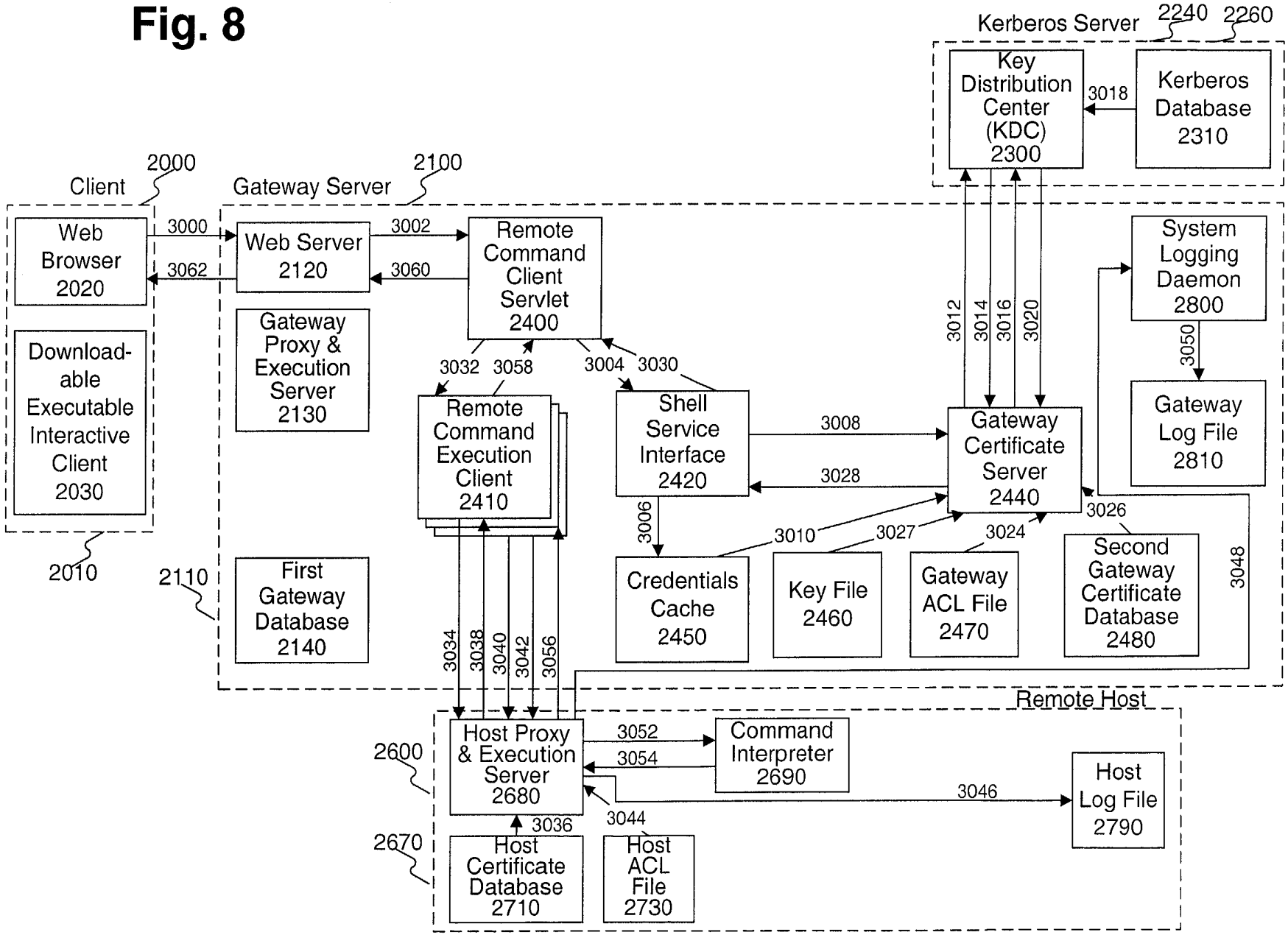


FIG. 9A

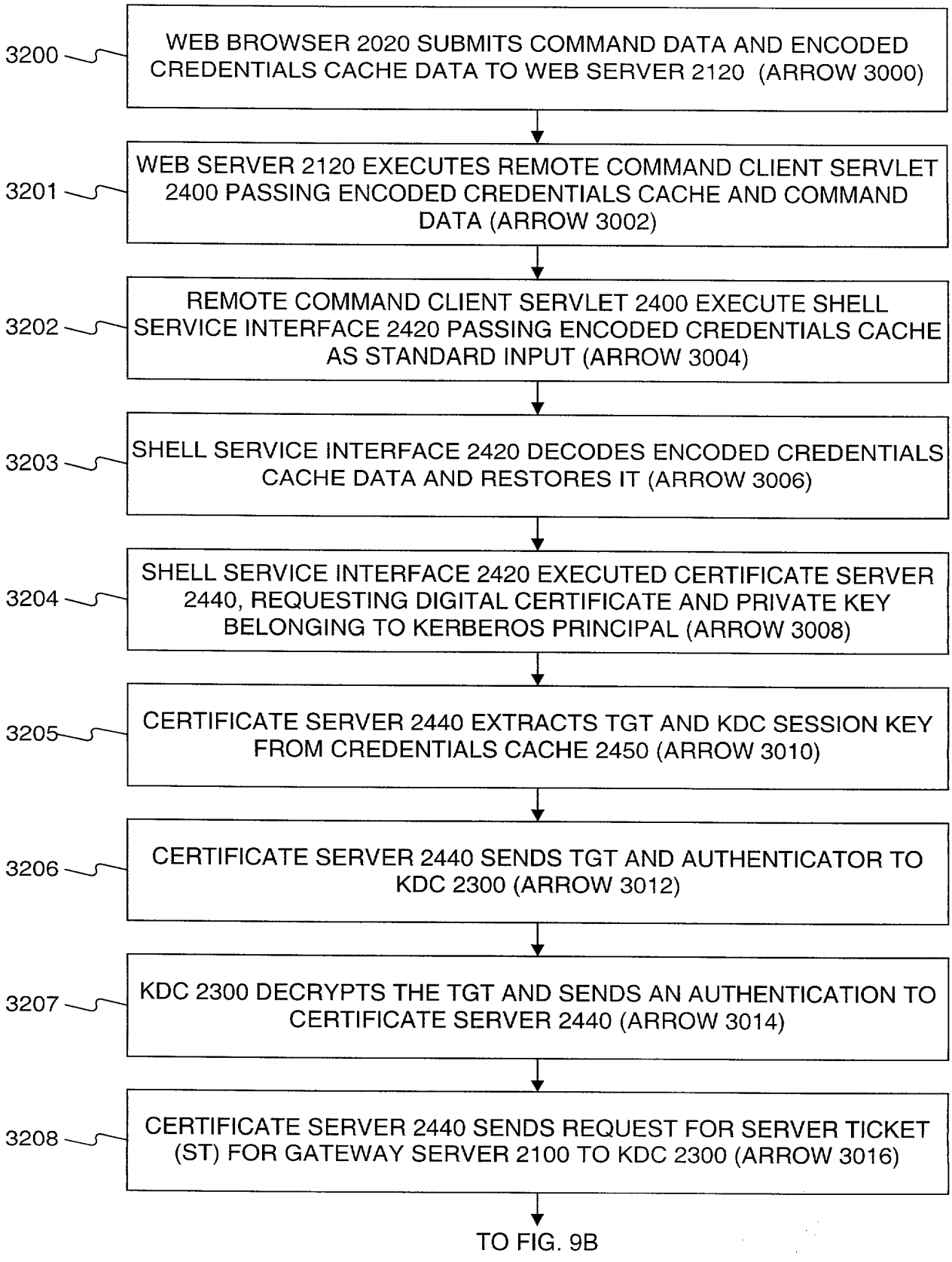

3200
WEB BROWSER 2020 SUBMITS COMMAND DATA AND ENCODED CREDENTIALS CACHE DATA TO WEB SERVER 2120 (ARROW 3000)
3201
WEB SERVER 2120 EXECUTES REMOTE COMMAND CLIENT SERVLET 2400 PASSING ENCODED CREDENTIALS CACHE AND COMMAND DATA (ARROW 3002)
3202
REMOTE COMMAND CLIENT SERVLET 2400 EXECUTE SHELL SERVICE INTERFACE 2420 PASSING ENCODED CREDENTIALS CACHE AS STANDARD INPUT (ARROW 3004)
3203
SHELL SERVICE INTERFACE 2420 DECODES ENCODED CREDENTIALS CACHE DATA AND RESTORES IT (ARROW 3006)
3204
SHELL SERVICE INTERFACE 2420 EXECUTED CERTIFICATE SERVER 2440, REQUESTING DIGITAL CERTIFICATE AND PRIVATE KEY BELONGING TO KERBEROS PRINCIPAL (ARROW 3008)
3205
CERTIFICATE SERVER 2440 EXTRACTS TGT AND KDC SESSION KEY FROM CREDENTIALS CACHE 2450 (ARROW 3010)
3206
CERTIFICATE SERVER 2440 SENDS TGT AND AUTHENTICATOR TO KDC 2300 (ARROW 3012)
3207
KDC 2300 DECRYPTS THE TGT AND SENDS AN AUTHENTICATION TO CERTIFICATE SERVER 2440 (ARROW 3014)
3208
CERTIFICATE SERVER 2440 SENDS REQUEST FOR SERVER TICKET (ST) FOR GATEWAY SERVER 2100 TO KDC 2300 (ARROW 3016)
TO FIG. 9B

FIG. 9B

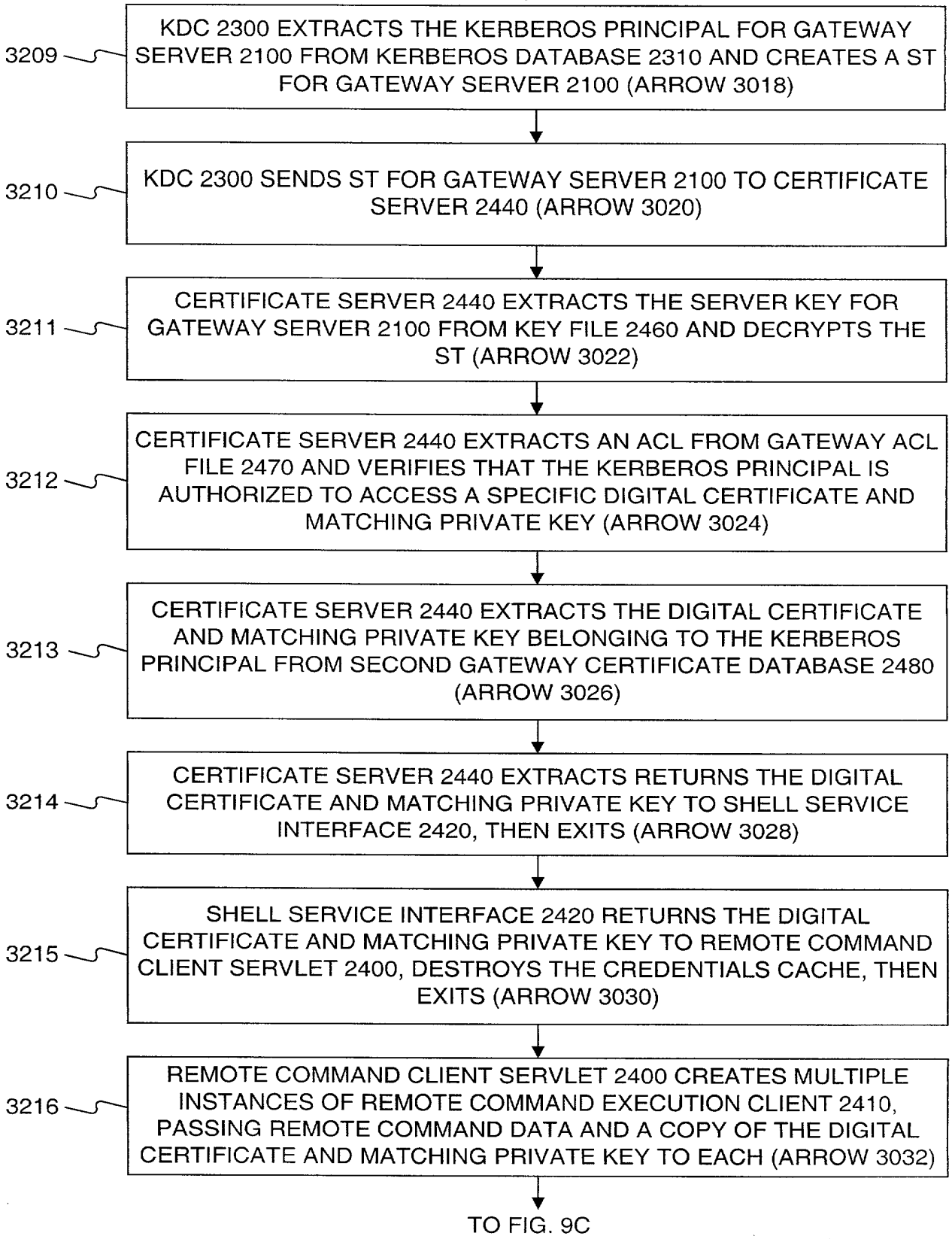

3209
KDC 2300 EXTRACTS THE KERBEROS PRINCIPAL FOR GATEWAY SERVER 2100 FROM KERBEROS DATABASE 2310 AND CREATES A ST FOR GATEWAY SERVER 2100 (ARROW 3018)
3210
KDC 2300 SENDS ST FOR GATEWAY SERVER 2100 TO CERTIFICATE SERVER 2440 (ARROW 3020)
3211
CERTIFICATE SERVER 2440 EXTRACTS THE SERVER KEY FOR GATEWAY SERVER 2100 FROM KEY FILE 2460 AND DECRYPTS THE ST (ARROW 3022)
3212
CERTIFICATE SERVER 2440 EXTRACTS AN ACL FROM GATEWAY ACL FILE 2470 AND VERIFIES THAT THE KERBEROS PRINCIPAL IS AUTHORIZED TO ACCESS A SPECIFIC DIGITAL CERTIFICATE AND MATCHING PRIVATE KEY (ARROW 3024)
3213
CERTIFICATE SERVER 2440 EXTRACTS THE DIGITAL CERTIFICATE AND MATCHING PRIVATE KEY BELONGING TO THE KERBEROS PRINCIPAL FROM SECOND GATEWAY CERTIFICATE DATABASE 2480 (ARROW 3026)
3214
CERTIFICATE SERVER 2440 EXTRACTS RETURNS THE DIGITAL CERTIFICATE AND MATCHING PRIVATE KEY TO SHELL SERVICE INTERFACE 2420, THEN EXITS (ARROW 3028)
3215
SHELL SERVICE INTERFACE 2420 RETURNS THE DIGITAL CERTIFICATE AND MATCHING PRIVATE KEY TO REMOTE COMMAND CLIENT SERVLET 2400, DESTROYS THE CREDENTIALS CACHE, THEN EXITS (ARROW 3030)
3216
REMOTE COMMAND CLIENT SERVLET 2400 CREATES MULTIPLE INSTANCES OF REMOTE COMMAND EXECUTION CLIENT 2410, PASSING REMOTE COMMAND DATA AND A COPY OF THE DIGITAL CERTIFICATE AND MATCHING PRIVATE KEY TO EACH (ARROW 3032)
TO FIG. 9C

FIG. 9C

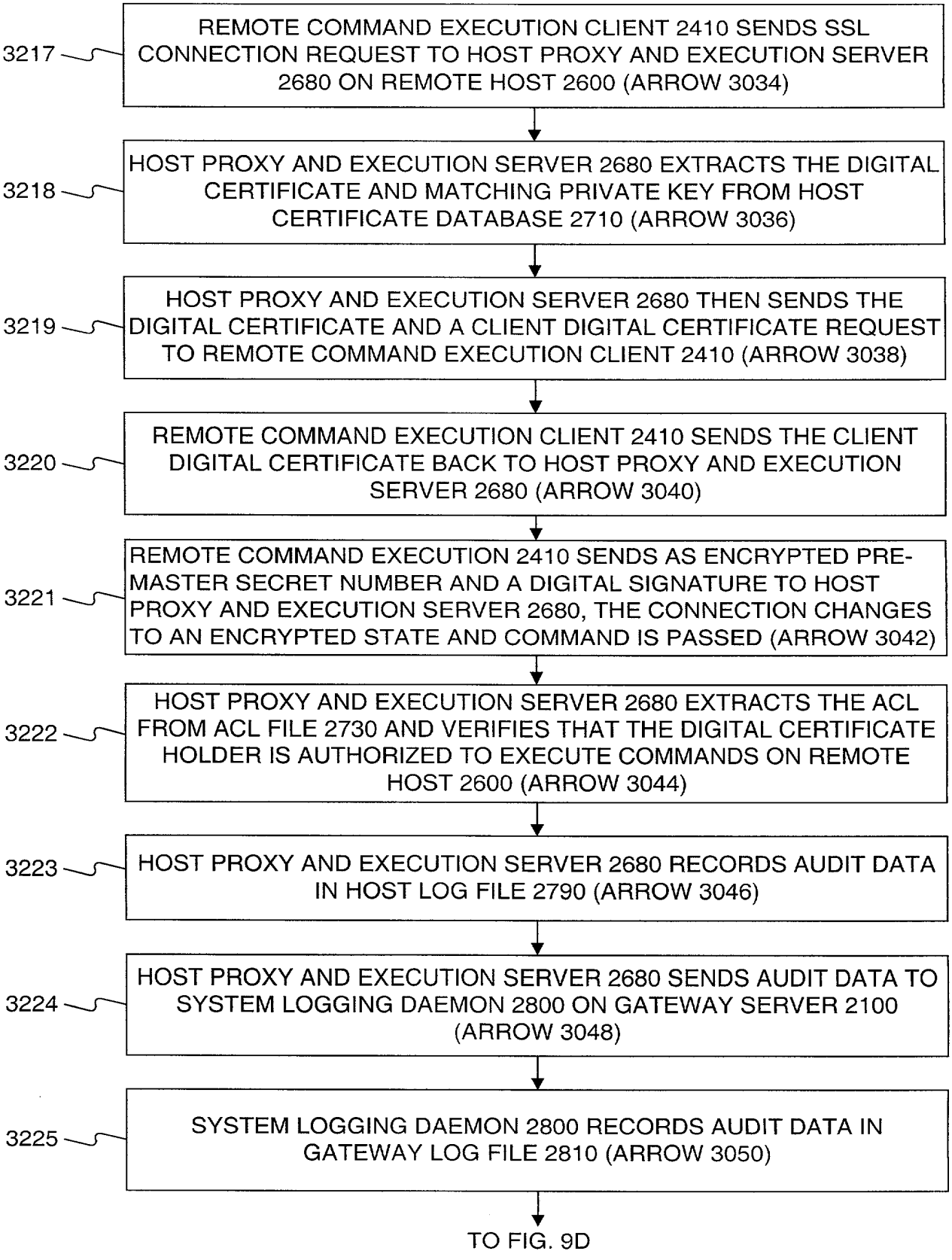
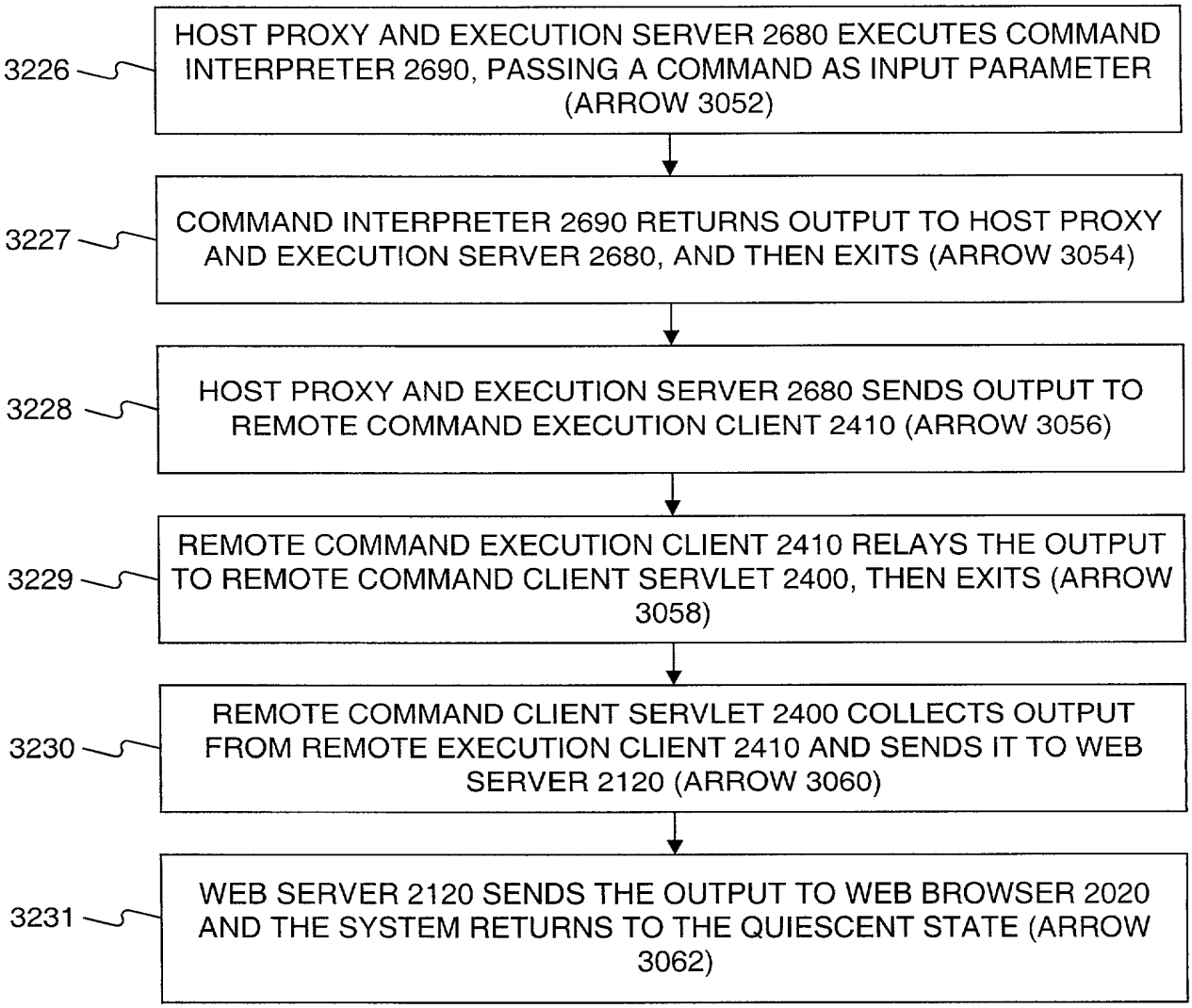

3217
REMOTE COMMAND EXECUTION CLIENT 2410 SENDS SSL CONNECTION REQUEST TO HOST PROXY AND EXECUTION SERVER 2680 ON REMOTE HOST 2600 (ARROW 3034)
3218
HOST PROXY AND EXECUTION SERVER 2680 EXTRACTS THE DIGITAL CERTIFICATE AND MATCHING PRIVATE KEY FROM HOST CERTIFICATE DATABASE 2710 (ARROW 3036)
3219
HOST PROXY AND EXECUTION SERVER 2680 THEN SENDS THE DIGITAL CERTIFICATE AND A CLIENT DIGITAL CERTIFICATE REQUEST TO REMOTE COMMAND EXECUTION CLIENT 2410 (ARROW 3038)
3220
REMOTE COMMAND EXECUTION CLIENT 2410 SENDS THE CLIENT DIGITAL CERTIFICATE BACK TO HOST PROXY AND EXECUTION SERVER 2680 (ARROW 3040)
3221
REMOTE COMMAND EXECUTION 2410 SENDS AS ENCRYPTED PRE-MASTER SECRET NUMBER AND A DIGITAL SIGNATURE TO HOST PROXY AND EXECUTION SERVER 2680, THE CONNECTION CHANGES TO AN ENCRYPTED STATE AND COMMAND IS PASSED (ARROW 3042)
3222
HOST PROXY AND EXECUTION SERVER 2680 EXTRACTS THE ACL FROM ACL FILE 2730 AND VERIFIES THAT THE DIGITAL CERTIFICATE HOLDER IS AUTHORIZED TO EXECUTE COMMANDS ON REMOTE HOST 2600 (ARROW 3044)
3223
HOST PROXY AND EXECUTION SERVER 2680 RECORDS AUDIT DATA IN HOST LOG FILE 2790 (ARROW 3046)
3224
HOST PROXY AND EXECUTION SERVER 2680 SENDS AUDIT DATA TO SYSTEM LOGGING DAEMON 2800 ON GATEWAY SERVER 2100 (ARROW 3048)
3225
SYSTEM LOGGING DAEMON 2800 RECORDS AUDIT DATA IN GATEWAY LOG FILE 2810 (ARROW 3050)
TO FIG. 9D

FIG. 9D


3226
HOST PROXY AND EXECUTION SERVER 2680 EXECUTES COMMAND INTERPRETER 2690, PASSING A COMMAND AS INPUT PARAMETER (ARROW 3052)
3227
COMMAND INTERPRETER 2690 RETURNS OUTPUT TO HOST PROXY AND EXECUTION SERVER 2680, AND THEN EXITS (ARROW 3054)
3228
HOST PROXY AND EXECUTION SERVER 2680 SENDS OUTPUT TO REMOTE COMMAND EXECUTION CLIENT 2410 (ARROW 3056)
3229
REMOTE COMMAND EXECUTION CLIENT 2410 RELAYS THE OUTPUT TO REMOTE COMMAND CLIENT SERVLET 2400, THEN EXITS (ARROW 3058)
3230
REMOTE COMMAND CLIENT SERVLET 2400 COLLECTS OUTPUT FROM REMOTE EXECUTION CLIENT 2410 AND SENDS IT TO WEB SERVER 2120 (ARROW 3060)
3231
WEB SERVER 2120 SENDS THE OUTPUT TO WEB BROWSER 2020 AND THE SYSTEM RETURNS TO THE QUIESCENT STATE (ARROW 3062)

FOREIGN DOCUMENT

Fig. 10

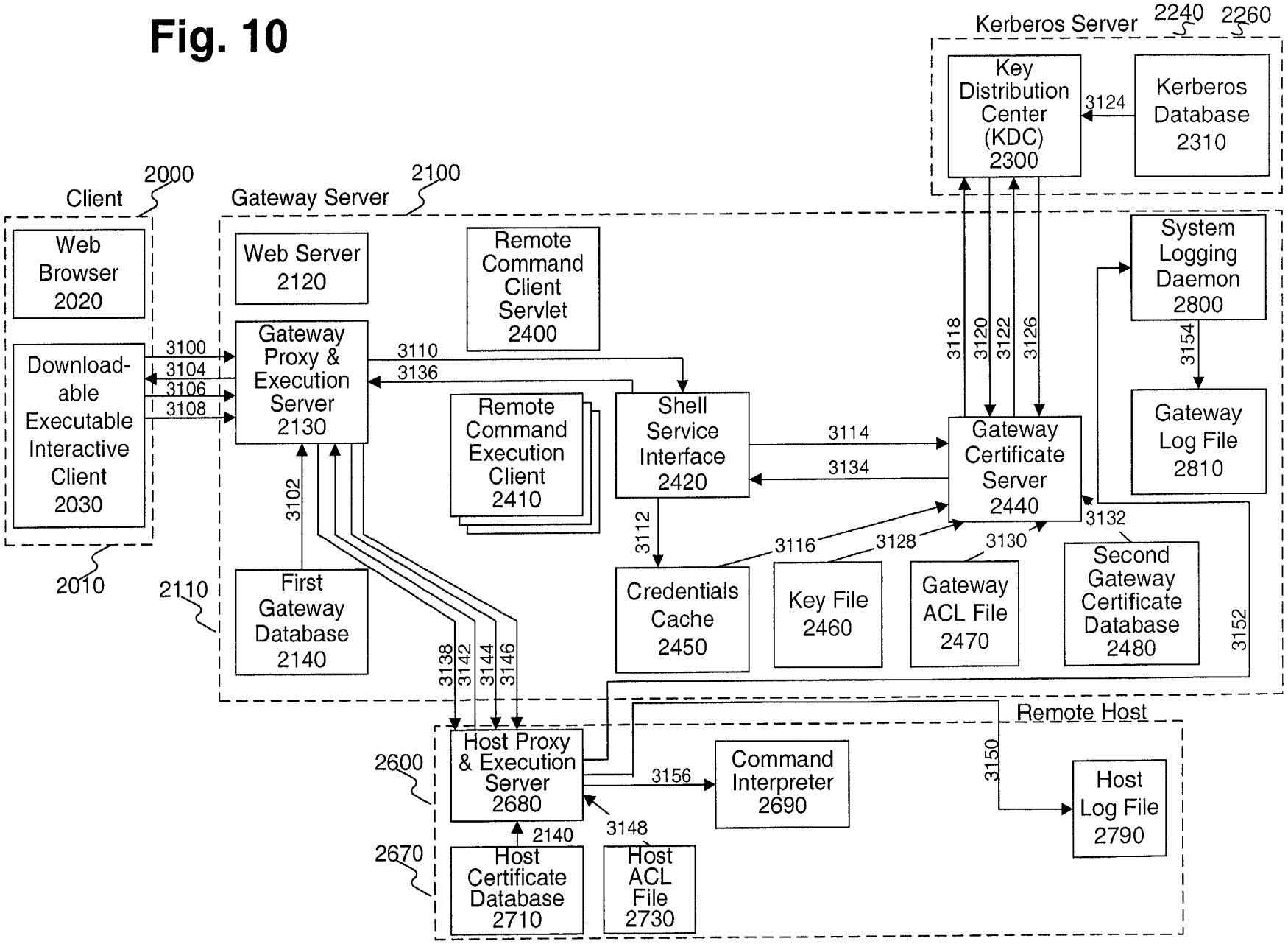
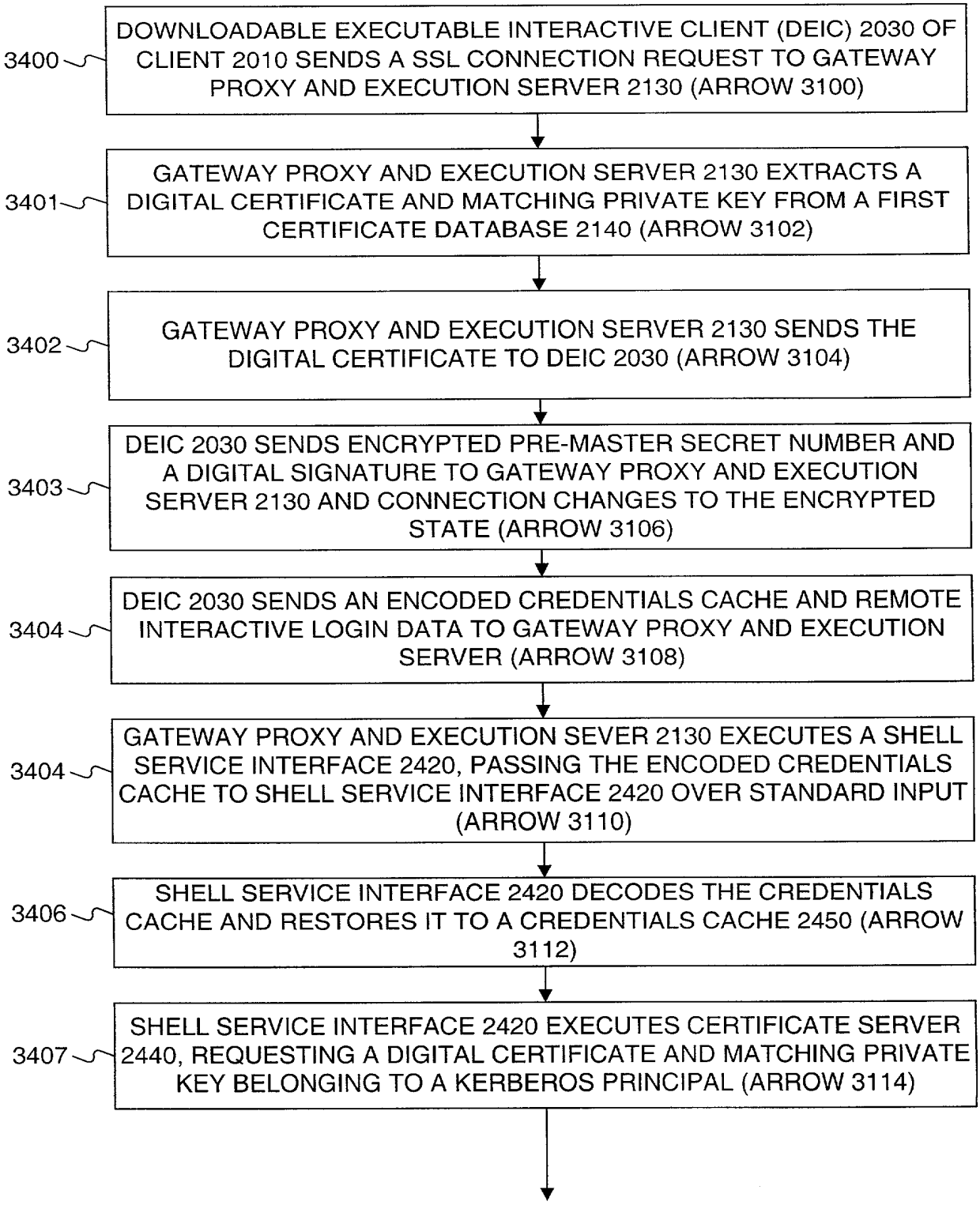
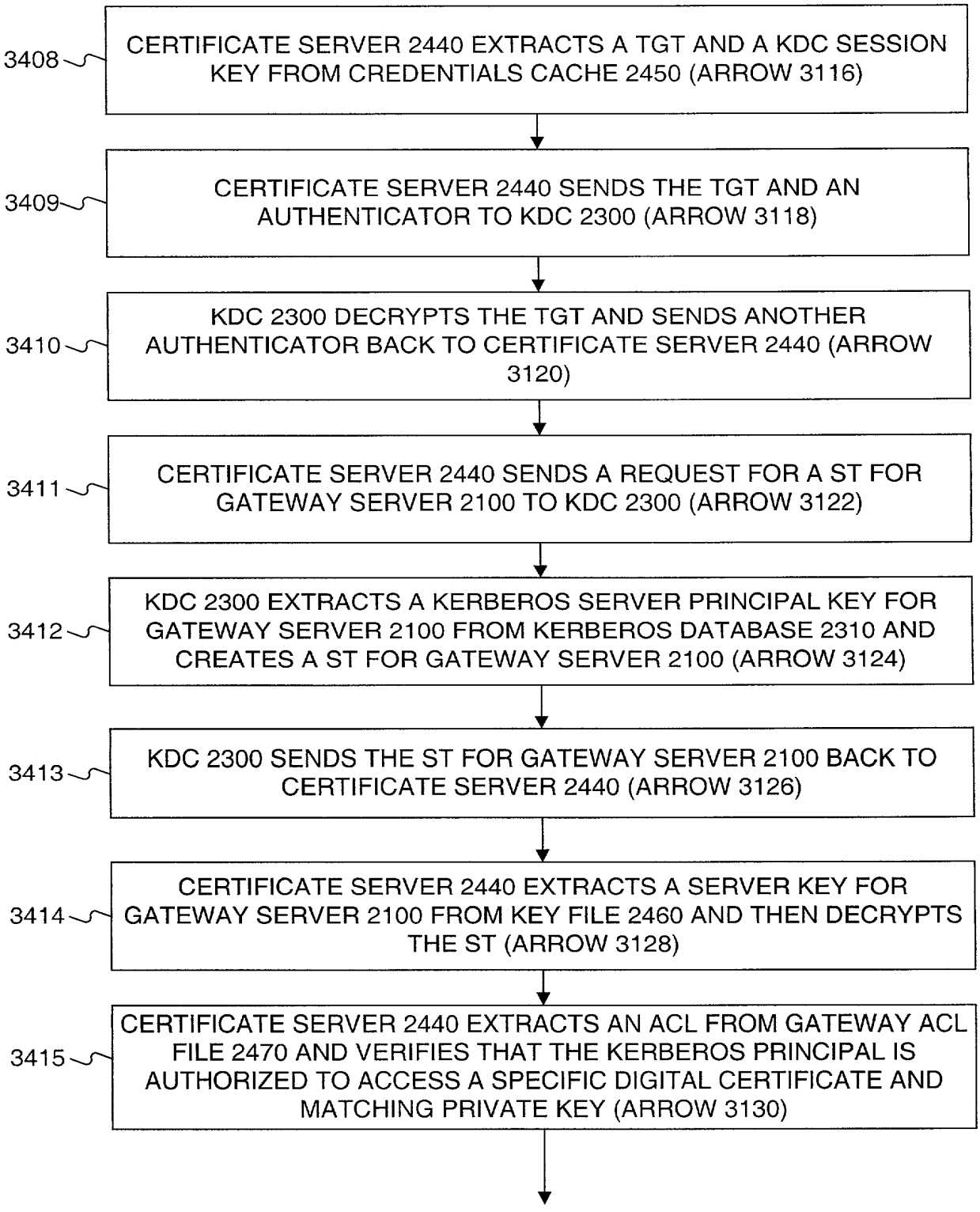


FIG. 11A



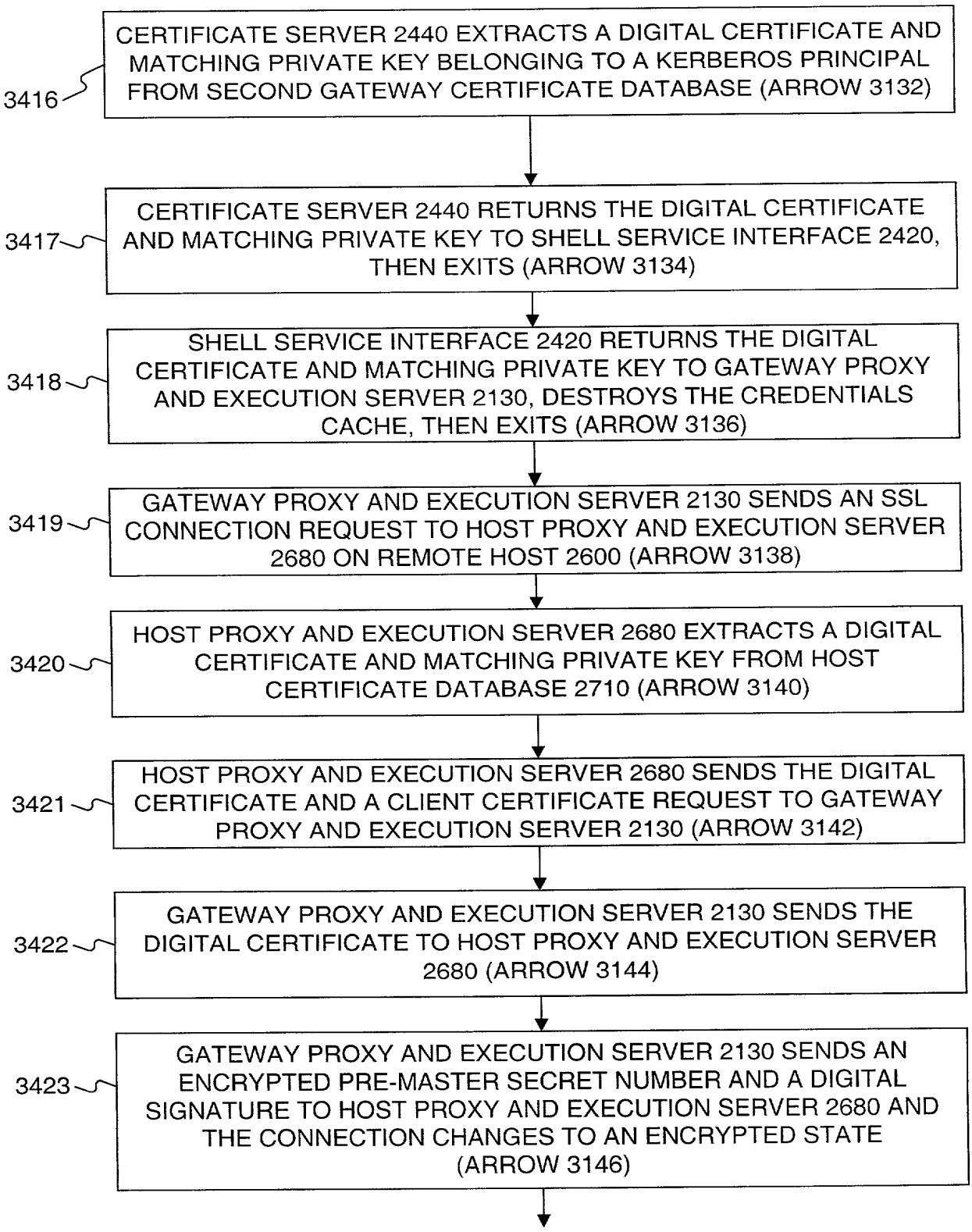
TO FIG. 11B

FIG. 11B



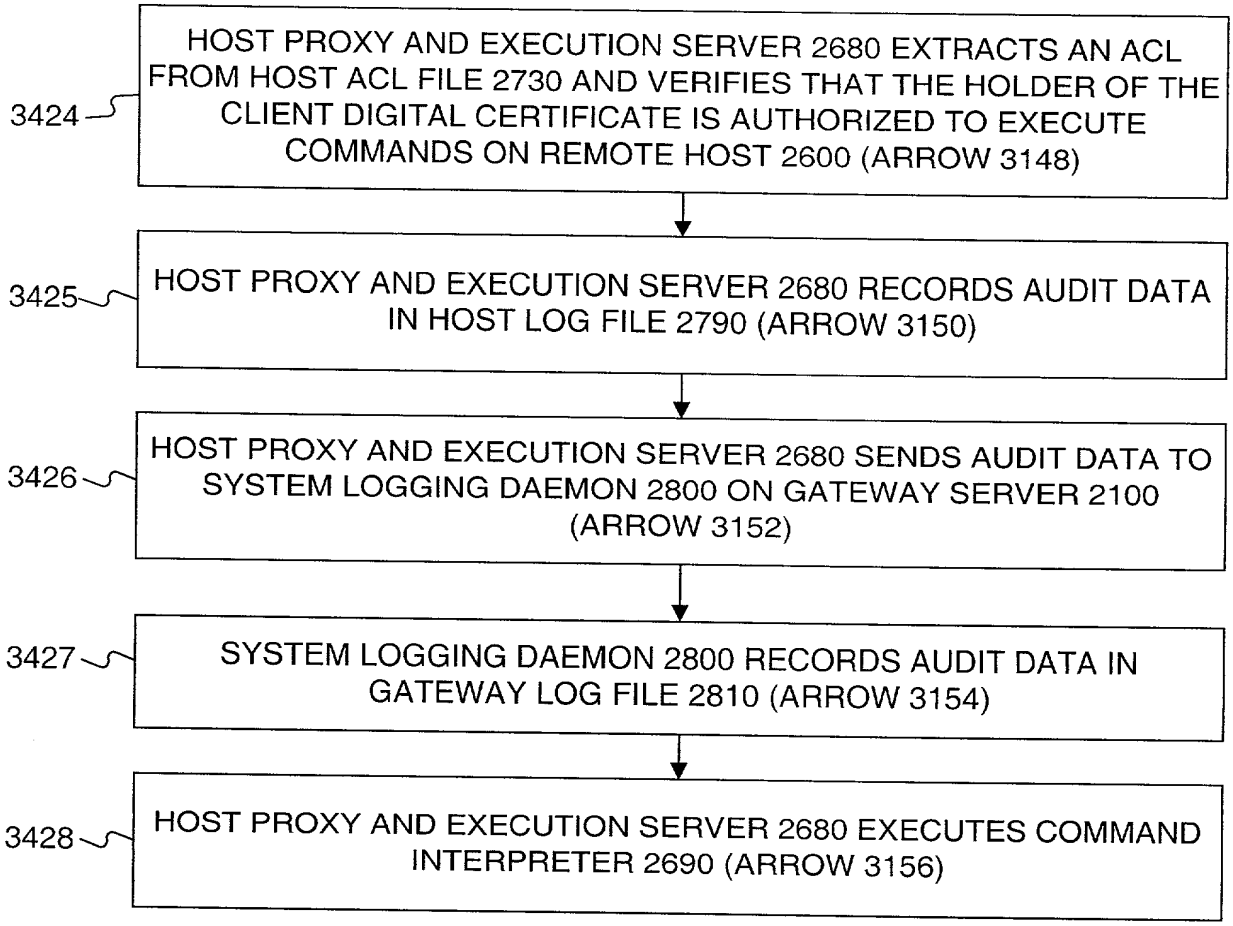
TO FIG. 11C

FIG. 11C



TO FIG. 11D

FIG. 11D


3424
HOST PROXY AND EXECUTION SERVER 2680 EXTRACTS AN ACL FROM HOST ACL FILE 2730 AND VERIFIES THAT THE HOLDER OF THE CLIENT DIGITAL CERTIFICATE IS AUTHORIZED TO EXECUTE COMMANDS ON REMOTE HOST 2600 (ARROW 3148)
3425
HOST PROXY AND EXECUTION SERVER 2680 RECORDS AUDIT DATA IN HOST LOG FILE 2790 (ARROW 3150)
3426
HOST PROXY AND EXECUTION SERVER 2680 SENDS AUDIT DATA TO SYSTEM LOGGING DAEMON 2800 ON GATEWAY SERVER 2100 (ARROW 3152)
3427
SYSTEM LOGGING DAEMON 2800 RECORDS AUDIT DATA IN GATEWAY LOG FILE 2810 (ARROW 3154)
3428
HOST PROXY AND EXECUTION SERVER 2680 EXECUTES COMMAND INTERPRETER 2690 (ARROW 3156)